About the Components

Switch - Layer 2 device

A switch basically has table that maps the MAC address of a device to the port of the switch. This table is called a CAM table. Using this table it can forward traffic without the traffic having to go through a router.

- Backbone/core/tandem switch is a switch with high capacity located in the physical core of the network. A backbone switch serves to interconnect edge switches. A core switch can sometimes operate on layer 3. Aggregation switches are usually connected to the core switch. It can have routing features as well. A normal port on a core switch might handle up to 10Gbps. You might connect the core switch to the aggregation switches using fiber, since those cables will carry a lot of traffic. The core switch usually server as a gateway to the WAN.
- Aggregation/distribution switch - basically a switch that servers as a connection between a core switch and an edge switch.
- Access/edge/normal switch - smaller capacity that are on the edges of the network. Usually used to connect end devices, like a computer.

Router - layer 3 device

A router is a layer 3 device. While a switch is a layer 2 device. Therefore you won't find subnets configured on a switch, but you will find it on a router. Since the router deals with layer 3 (IP)

VLAN

A VLAN is fundamentally a layer 2 virtual lan. This means that it does not concern IP-addresses, as one might initially think. We usually think of a VLAN as a subnet. But a VLAN is a layer 2 segmentation, and subnet is a layer 3. However, it is common with a one-to-one relationship between a VLAN and a subnet. That is: `VLAN 10` is related to `192.168.11.1/24`. This is why you might enter a cisco switch and you won't find subnet information.

On cisco router `show vlans` will show the IP-address. On a switch however `show vlans` does not exist.

A VLAN is simply a tag that is added to each ethernet frame. That is why a switch does not really need to look at traffic above the ethernet frame. This tag is the `IEEE 802.1Q` header (also known as `Dot1q`) of the ethernet frame. However if you sniff the traffic on your computer you will likely not see the Dot1q tag, because it is removed when sent to the end user. It is only used between switches, I think.

A basic switch that does not have VLANs enabled will have a default VLAN enabled that contains all the ports of the switch. The default VLAN usually uses the ID 1.

A trunk is a network link that carries multiple VLANs. In cisco world the word channel is sometimes used to say trunk.

Protocols and terminology

HSRP

Hot Standby Router Protocol (HSRP) is a cisco protocol which provides redudancy for a local subnet. In HSRP two or more routers gives an illusion of one virtual router. It allows you to configure one router to be the active router, and others to be the standby router. All routers in a single HSRP group share a MAC address and IP address. The active router is responsible for forwarding the traffic, if that router fails the standby router takes over.

SNMP - Simple Network Management Protocol

SNMP is a protocol used to manage and monitor network devices. SNMP is used to monitor your network. It does this by sending out messages to devices on the network that speak SNMP. These are SNMP get-requests.

Managed device - the device that can be queried for information.

Agent - the service/agent running on a device that collects the data that can be queried over SNMP.

Network Managemet station

VRF - Virtual Routing and Forwarding

VRF is used to create many virtual routing tables. A typical example would be ISP's using same router to route traffic for various customers and configure VRF to separate the various customer traffics with the router.

Some Network Attacks

VLAN hopping using DTP

Background

A switch has a number of ports. Those ports can be either **access port** or **trunking port**. An access port is usually used when connecting a host to the switch. Just like a regular computer. Each access port is assigned one VLAN, and only one. A trunking port is used when conneting two switches or connecting a switch and a router. Trunking ports allow traffic from multiple lans. A trunk port can be configured manually. But there is also a protocol that can do this over the network, Dynamic Trunk Protocol.

So, as you can understand the attack is to transform the access port that you are connected to into a trunking port, in order to be able to access other VLANS.

So an attack can be performed against ports that are configured to be **dynamic desirable**, **dynamic auto**, or **trunk** mode.

A port can be in a number of different states:

- **AUTO** - if the port is configured to listen for DTP frames it can convert the port to a trunk port of the other switch decides sends the DTP frame.
- **DESIRABLE** - DTP is spoken to the neighbor switch with the desire that the other switch form a trunk.
- **ON** -

Attack

Since it is a protocol an attacker can simply send a DTP packet and instruct the switch to becomes a trunk. If an attacker is successfull it will turn that port into a trunk.

Cisco insecure password type

Background

There exists multiple password types in Cisco.

The passwords can be stored in a number of different ways, or Types as cisco calls them. Type 0 is plaintext. Etc. Type 9 is the secure version.

Passwords are stored in configurations and can be read with commands like

```
show running-config
```

Username

Check that it is using type 9.

```
show running-config | incl username
```

Check that it is using "secret 9"

HSRP

Check for usage of encrypted password for HSRP. ALthough this is pretty shitty security.

```
show standby
```

SNMP

TACTACS

Look for the tactac-configuration. Check that it is key 7.

```
 show running-config
server-private 1.1.1.1 key 7 45weg45345345345
```

BGP

```

```

Weak password

In some protocols a password is used. You need to make sure that the password is not superweak. If you run

```
show running-config
```

You can check for passwords and see if they are really weak. They might be encrypted, but if they are of `type 7` they can easily be decrypted.

BGP For example, with BGP it is possible to configure BGP peer authentication. BGP authentication can be used by entering the neighbor command in cisco.

It will look something like this:

```
 show running-config
neighbor 8.8.9.1 password 7 1511021F0725
```

`Password 7` means that it is is encrypted. But it can easily be decrypted by anyone. It is just to store the password in non-plaintext. But the password will be hashed into MD5 when used with BGP. So if it uses `password 7` there is nothing really to complain about, but what you can do is simply decrypt it and check that the password is not very weak.

You can do this with this script: https://github.com/theevilbit/ciscot7/blob/master/ciscot7.py

SNMP

Community string is just another word for password. The default community string is public or private. This should be set to something else.

```
show running-config | incl snmp
```

SNMP Configurations

Check for weak/default passwords

How to do that can be found in the section about weak passwords.

Check for read write

CIS 1.5.4

SNMP should not be used in Read write mode unless absolutley necessary.

Check for RW whe you run the following command.

```
show run | incl snmp-server community
```

Check for ACL on SNMP

CIS 1.5.5

Exploiting spanning-tree protocol

Background

STP is a layer 2 protocol. STP is used to prevent layer 2 switching loops. It does so by shutting down redudant links. So say you have two links between two switches. STP makes sure that you in fact only have one, so that a packet won't enter into a loop. Redudant links are however important to server at a backup. If two links are active at the same time it will create a loop.

If a switch recive a unicast, multicast or broadcast. These frames will be forwarded to all ports on the switch except for the port it recieved the frame on. This means that the frame will be sent to another switch, which will send it back to the first swich. Thereby creating a loop. An infinite loop is sometimes called a **broadcast storm**.

STP activly monitors all links on the network. It uses an algorithm called spanning-tree algorithm in order to find redudant links. The protocol disabled redudant links.

STP decides on which switch should be the root bridge. It does this by looking at bridge priority value. On cisco this is always 32768.

- Root Bridge - The switch that is the root in the spanning tree
- Root Port - All switches choose a root port. which is the port with the lowest cost to the root bridge.

Ports that do not participate in the tree are blocked.

In order to implement STP you need to specify your most centralized switch to be the root. This is often the core/backbone switch.

Exploit

So since STP is just a protocol that switches uses, and there is no authentication you might see where this is going. An attacker can simply set itself to become the root bridge, this means that the other switches would forward traffic to your host. An attacker can flood the network with BPDU packets advertising that your own host has the lowest bridge cost.

You can also advertise your link of having a lower cost. This will direct traffic through you.

These attacks can be performed with `yersinia`. You should probably look up how much traffic might be sent over your link.

Note that you might bring down the network if you perform this attack.

How to check for

```
show spanning-tree summary
```

Root Guard

Checking for root guard has to be done on each port

```
 show interface summary
show spanning-tree interface TenGigabitEthernet1/0/4 detail

This syntax is also possible:
show spanning-tree interface Te1/0/4 detail
```

If it says "Root guard is enabled on the port" Root guard is enabled, if it doesn't say anything I think it means that is is not enabled.

Recommendation

For Cisco devices that are primarpily two defence mechanisms against these attacks: Root Guard and BPDU Guard. BPDU guard is enabled on a switch, and root guard on a port basis.

References

https://flylib.com/books/en/3.418.1.75/1/

Patch level

Background

Cisco devices are very prone to security issues.

How to check

Check which version of the OS the device is running.

```
show version
```

ARP spoofing / ARP poisoning

Background

One classic attack is called ARP poisoning.

Recommendation

Enable Dynamic ARP Inspection

Rouge DHCP attack

Background

Recommendation

Enable DHCP snooping

IP/MAC spoofing

Background

Recommendation

Can be prevented by IP source guard - in Cisco

IPv6 Man in the middle

Background

Recommendation

IPv6 Router Advertisment Guard can be used to protect.

CAM overflow attack

Background

Switches work by building a reference table between a switch port and a MAC address. Based on the destination MAC address the switch knows which port to send the traffic to.

This table is called context-addressable memory (CAM) table.

The switch can only hold a limited amount of MAC addresses in this table. An attacker can abuse this by performing a CAM overflow attack. The attacker mimics the existence of thousdands of random MAC addresses on one (or more) ports. The switch enters all these MAC addresses in the CAM table, and eventually the table overflows.

Since the table is full the switch doesn't can't know where to send other traffic, legitimate traffic. So the switch turns into a hub, and sends the traffic out to all hosts that are connected to the switch. This allows an attacker to sniff traffic performed by other users.

DHCP starvation attacks